CLAIMS

1. An information recording/playback system for recording and playing back information, comprising:

an authentication data recording control part which provides control of detecting random pattern information based on random physical phenomena from a random-pattern-information recording part used for recording random pattern information based on random physical phenomena, creating medium identification information from the random pattern information, and recording, as authentication data, the medium identification information in an authentication data recording part on the information recording medium;

an authentication processing part which detects the random pattern information from the random-pattern-information recording part, creates medium-identification-information verification data from the random pattern information, reads authentication data from the authentication data recording part on the information recording medium, and performs authentication processing for the information recording medium based on medium-identification-information verification data created from the random pattern information and based on the authentication data; and

an information recording/playback control part which provides control of recording information on an information recording medium and playing back information from an information recording medium based on an authentication result

from the authentication processing part.

2. The information recording/playback system according to claim 1, wherein there is further provided an encryption part which encrypts information by using medium identification information from an information recording medium authenticated by the authentication processing, and

wherein the information recording/playback control part provides control of recording information encrypted by the encryption part on the authenticated information recording medium.

3. The information recording/playback system according to claim 2, wherein the information recording/playback control part provides control of recording encrypted information and the encryption key used for information encryption on the authenticated information recording medium.

4. The information recording/playback system according to claim 3, wherein the encryption part encrypts information using the encryption key and encrypts the encryption key used for information encryption by using medium identification information on an information recording medium authenticated by the authentication processing,

wherein the information recording/playback control part provides control of recording information encrypted with the encryption key and the encrypted encryption key on the authenticated information recording medium.

5. The information recording/playback system according to claim 2, wherein the

encryption part creates an encryption key used for the information encryption by using medium identification information on an information recording medium authenticated by the authentication processing.

6. The information recording/playback system according to claim 1, wherein there is further provided a decryption part for decrypting information by using medium identification information on an information recording medium authenticated by the authentication processing,

wherein the information recording/playback control part provides control of reading encrypted information from the authenticated information recording medium, and

wherein the decryption part decrypts encrypted information read by the information recording/playback control part from an information recording medium by using medium identification information on an information recording medium authenticated by the authentication processing.

7. The information recording/playback system according to claim 6, characterized in that the information recording/playback control part provides control of reading encrypted information and the encryption key used for information encryption from the authenticated information recording medium.

8. The information recording/playback system according to claim 7, wherein the information recording/playback control part provides control of reading encrypted information and the encrypted encryption key from the information recording medium,

and

wherein the decryption part decrypts a read and encrypted encryption key by using medium identification information on an information recording medium authenticated by the authentication processing and decrypts encrypted information by using the encryption key which was encrypted and information thereof is decrypted.

9. The information recording/playback system according to claim 1, wherein the authentication data recording control part records, as authentication data, the medium identification information together with a digital signature of a recording person who recorded the medium identification information in the authentication data recording part on the information recording medium.

10. An information recording/playback system according to claim 9, wherein the authentication data recording control part records a digital signature for a manufacturer of the information recording medium as a digital signature for a recording person who recorded the medium identification information.

11. An information recording apparatus for recording information on an information recording medium including a random-pattern-information recording part for recording random pattern information based on random physical phenomena and an authentication data recording part for storing, as authentication data, medium identification information generated according to random pattern information detected from the random-pattern-information recording part, wherein the information recording apparatus is , comprising:

a random-pattern-information detection part which detects random pattern information from a random-pattern-information recording part on an information recording medium;

a verification data creation part which creates medium-identification-information verification data from random pattern information detected by the random-pattern-information detection part;

an authentication processing part which reads authentication data from an authentication data recording part on an information recording medium, performs authentication processing for an information recording medium based on medium-identification-information verification data created by the verification data creation part and based on the authentication data, and controls whether to write information onto an information recording medium based on an authentication result; and

a recording control part which provides control of recording information on an information recording medium.

12. The information recording apparatus according to claim 11, wherein there is further provided an encryption part which encrypts information by using medium identification information on an information recording medium authenticated by the authentication processing, and

wherein the recording control part provides control of recording information encrypted by the encryption part on the authenticated information recording medium.

13. The information recording apparatus according to claim 12, wherein the recording control part provides control of recording encrypted information and the encryption key used for information encryption on the authenticated information recording medium.

14. The information recording apparatus according to claim 13, wherein the encryption part encrypts information by using the encryption key and encrypts the encryption key used for information encryption by using medium identification information on an information recording medium authenticated by the authentication processing, and

wherein the recording control part provides control of recording information encrypted with the encryption key and the encrypted encryption key on the authenticated information recording medium.

15. The information recording apparatus according to claim 12, characterized in that the encryption part creates an encryption key used for the information encryption by using medium identification information on an information recording medium authenticated by the authentication processing.

16. The information recording apparatus according to claim 11, wherein that the authentication processing part verifies validity of the medium identification information with respect to an information recording medium which records, as authentication data, the medium identification information together with a digital signature of a recording person who recorded the medium identification information

based on the recording person's digital signature, and performs authentication processing with respect to an information recording medium based on medium-identification-information verification data created by the verification data creation part and based on verified valid medium identification information.

17. The information recording apparatus according to claim 16, wherein the authentication processing part verifies validity of the medium identification information with respect to an information recording medium which records a digital signature of a manufacturer for the information recording medium as a digital signature for a recording person of the medium identification information based on the manufacturer's digital signature.

18. The information recording apparatus according to claim 16, wherein the authentication processing part performs authentication processing with respect to an information recording medium which records a revocation list about a recording person together with the authentication data based on the revocation list.

19. The information recording apparatus according to claim 18, wherein the authentication processing part has a storage part for storing the revocation list, stores a revocation list recorded on an information recording medium in the storage part when this revocation list is valid and is newer than the revocation list stored in the storage part, and performs authentication processing based on the revocation list stored in the storage part.

20. An information playback apparatus for playing back information from an

information recording medium including a random-pattern-information recording part for recording random pattern information based on random physical phenomena and an authentication data recording part for storing, as authentication data, medium identification information created according to random pattern information detected from the random-pattern-information recording part, wherein the information playback apparatus,

a random-pattern-information detection part which detects random pattern information from the random-pattern-information recording part on the information recording medium;

a verification data creation part which creates medium-identification-information verification data from random-pattern-information detected by the random-pattern-information detection part;

an authentication processing part which reads authentication data from the authentication data recording part and performs authentication processing with respect to an information recording medium based on medium-identification-information verification data created by the verification data creation part and based on the authentication data; and

a playback control part which provides control of reading information from an information recording medium.

21. The information playback apparatus according to claim 20, wherein the playback control part provides control of reading encrypted information from the authenticated

information recording medium, and

wherein the decryption part decrypts encrypted information read from the information recording medium by the playback control part by using medium identification information on the information recording medium authenticated by the authentication processing.

22. The information playback apparatus according to claim 21, wherein the playback control part provides control of reading encrypted information and an encryption key used for the information encryption from the authenticated information recording medium.

23. The information playback apparatus according to claim 22, wherein the playback control part provides control of reading encrypted information and the encrypted encryption key from the authenticated information recording medium, and

wherein the decryption part decrypts a read and encrypted encryption key by using medium identification information on an information recording medium authenticated by the authentication processing and decrypts encrypted information by using the encryption key which was encrypted and information thereof is decrypted.

24. The information playback apparatus according to claim 20, wherein the authentication processing part verifies validity of the medium identification information with respect to an information recording medium which records, as authentication data, the medium identification information together with a digital signature of a recording person who recorded the medium identification information

based on the recording person's digital signature, and performs authentication processing with respect to the information recording medium based on medium-identification-information verification data created by the verification data creation part and based on verified valid medium identification information.

25. The information playback apparatus according to claim 24, wherein the authentication processing part verifies validity of the medium identification information with respect to an information recording medium which records a digital signature of a manufacturer for the information recording medium as a digital signature for a recording person of the medium identification information based on the manufacturer's digital signature.

26. The information playback apparatus according to claim 24, wherein the authentication processing part performs authentication processing with respect to an information recording medium which records a revocation list about a recording person together with the authentication data based on the revocation list.

27. The information playback apparatus according to claim 26, wherein the authentication processing part has a storage part for storing the revocation list, stores a revocation list recorded on an information recording medium in the storage part when this revocation list is valid and is newer than the revocation list stored in the storage part, and performs authentication processing based on the revocation list stored in the storage part.

28. An authentication data recording apparatus for recording authentication

information on an information recording medium, comprising:

a random-pattern-information detection part which detects random pattern information from a random-pattern-information recording part on an information recording medium for storing random pattern information based on random physical phenomena;

a medium identification information creation part which creates medium identification information from the random pattern information detected by the random-pattern-information detection part; and

an authentication data recording control part which provides control of recording, as authentication data, the medium identification information created by the medium identification information creation part in an authentication data recording part on the information recording medium.

29. The authentication data recording apparatus according to claim 28, wherein the authentication data recording control part records, as authentication data, the medium identification information together with a digital signature for a recording person of the medium identification information in an authentication data recording part on the information recording medium.

30. The authentication data recording apparatus according to claim 28, characterized in that the authentication data recording control part records a digital signature for a manufacturer of the information recording medium as a digital signature for a recording person of the medium identification information.

31. The authentication data recording apparatus according to claim 28, wherein the authentication data recording control part records a revocation list about a manufacturer together with the authentication data in an authentication data recording part on the information recording medium.

32. An authentication processing apparatus for performing authentication processing with respect to an information recording medium, comprising:

a random-pattern-information detection part which detects random pattern information from a random-pattern-information recording part on the information recording medium;

a verification data creation part which creates medium-identification-information verification data from random pattern information detected by the random-pattern-information detection part; and

an authentication processing part which reads authentication data from an authentication data recording part on the information recording medium and performs authentication processing with respect to the information recording medium based on medium-identification-information verification data created by the verification data creation part and based on the authentication data.

33. The authentication processing apparatus according to claim 32, wherein the authentication processing part verifies validity of the medium identification information with respect to an information recording medium which records, as authentication data, the medium identification information together with a digital

signature of a recording person who recorded the medium identification information based on the recording person's digital signature, and performs authentication processing with respect to the information recording medium based on medium-identification-information verification data created by the verification data creation part and based on verified valid medium identification information.

34. The authentication processing apparatus according to claim 33, wherein the authentication processing part verifies validity of the medium identification information with respect to an information recording medium which records a digital signature of a manufacturer for the information recording medium as a digital signature for a recording person of the medium identification information based on the manufacturer's digital signature.

35. The authentication processing apparatus according to claim 33, wherein the authentication processing part performs authentication processing with respect to an information recording medium which records a revocation list about a recording person together with the authentication data based on the revocation list.

36. The authentication processing apparatus according to claim 35, wherein the authentication processing part has a storage part for storing the revocation list, stores a revocation list recorded on an information recording medium in the storage part when this revocation list is valid and is newer than the revocation list stored in the storage part, and performs authentication processing based on the revocation list stored in the storage part.

37. The authentication processing apparatus according to claim 35, wherein the authentication processing part has a storage part, stores a recording person's identification information and a public key thereof for a manipulated information recording medium together with a revocation flag, updates the revocation flag using a new revocation list, and performs authentication processing based on the revocation list stored in the storage part.

38. An information recording/playback method for recording and playing back information, comprising:

an authentication data recording control process which provides control of detecting random pattern information based on random physical phenomena from a random-pattern-information recording part for recording random pattern information based on random physical phenomena on an information recording medium, creating medium identification information from the random pattern information, and recording, as authentication data, the medium identification information in an authentication data recording part on the information recording medium;

an authentication process which detects the random pattern information from the random-pattern-information recording part, creates medium-identification-information verification data from the random pattern information, reads authentication data from the authentication data recording part on the information recording medium, and performs authentication processing with respect to the information recording medium based on

medium-identification-information verification data created from the random pattern information and based on the authentication data; and

an information recording/playback control process which provides control of recording information on an information recording medium and playing back information from an information recording medium based on an authentication result from the authentication processing process.

39. The information recording/playback method according to claim 38, wherein there is further provided an encryption process which encrypts information using medium identification information from an information recording medium authenticated by the authentication processing, and

wherein the information recording/playback control process provides control of recording information encrypted by the encryption process on the authenticated information recording medium.

40. The information recording/playback method according to claim 39, wherein the information recording/playback control process provides control of recording encrypted information and the encryption key used for information encryption on the authenticated information recording medium.

41. The information recording/playback method according to claim 40, wherein the encryption process encrypts information using the encryption key and encrypts the encryption key used for information encryption using medium identification information on an information recording medium authenticated by the authentication

processing, and

wherein the information recording/playback control process provides control of recording information encrypted with the encryption key and the encrypted encryption key on the authenticated information recording medium.

42. The information recording/playback method according to claim 39, wherein the encryption process creates the encryption key used for information encryption by using medium identification information on an information recording medium authenticated by the authentication processing.

43. The information recording/playback method according to claim 38, wherein the information recording/playback control process provides control of reading encrypted information from the authenticated information recording medium, and

wherein the decryption process decrypts encrypted information read by the information recording/playback control process from an information recording medium by using medium identification information on an information recording medium authenticated by the authentication processing.

44. The information recording/playback method according to claim 43, wherein the information recording/playback control process provides control of reading encrypted information and the encryption key used for information encryption from the authenticated information recording medium.

45. The information recording/playback method according to claim 44, wherein the information recording/playback control process provides control of reading encrypted

information and the encrypted encryption key from the authenticated information recording medium, and

wherein the decryption process decrypts a read and encrypted encryption key by using medium identification information on an information recording medium authenticated by the authentication processing and decrypts encrypted information by using the encryption key which was encrypted and information thereof is decrypted.

46. The information recording/playback method according to claim 38, wherein the authentication data recording control process records, as authentication data, the medium identification information together with a digital signature for a recording person of the medium identification information in an authentication data recording part on the information recording medium.

47. The information recording/playback method according to claim 46, wherein the authentication data recording control process records a digital signature for a manufacturer of the information recording medium as a digital signature for a recording person of the medium identification information.

48. An information recording method for recording information on an information recording medium including: a random-pattern-information recording part which records random pattern information based on random physical phenomena; and an authentication data recording part which stores, as authentication data, medium identification information created according to random pattern information detected from the random-pattern-information recording part, wherein the information

recording method, comprising:

a random-pattern-information detection process which detects random pattern information from a random-pattern-information recording part on an information recording medium;

a verification data creation process which creates medium-identification-information verification data from random pattern information detected by the random-pattern-information detection process;

an authentication process which reads authentication data from the authentication data recording part on an information recording medium, performs authentication processing for an information recording medium based on medium-identification-information verification data created by the verification data creation process and based on the authentication data, and controls whether to enable writing information onto an information recording medium based on an authentication result; and

a recording control process which provides control of recording information onto an information recording medium.

49. The information recording method according to claim 48, wherein there is further provided an encryption process which encrypts information using medium identification information from an information recording medium authenticated by the authentication processing, and

wherein the recording control process provides control of recording information

authenticated by the encryption process on the authenticated information recording medium.

50. The information recording method according to claim 49, characterized in that the recording control process provides control of recording encrypted information and the encryption key used for information encryption on an authenticated information recording medium.

51. The information recording method according to claim 50, wherein the encryption process encrypts information using the encryption key and encrypts the encryption key used for information encryption using medium identification information on an information recording medium authenticated by the authentication processing, and

wherein the recording control process provides control of recording information encrypted with the encryption key and the encrypted encryption key on the authenticated information recording medium.

52. The information recording method according to claim 49, wherein the encryption process creates an encryption key used for the information encryption by using medium identification information on an information recording medium authenticated by the authentication processing.

53. An information recording method according to claim 48, characterized in that the authentication process verifies validity of the medium identification information with respect to an information recording medium which records, as authentication data, the medium identification information together with a digital signature of a recording

person who recorded the medium identification information based on the recording person's digital signature, and performs authentication processing with respect to the information recording medium based on medium-identification-information verification data created by the verification data creation process and based on verified valid medium identification information.

54. The information recording method according to claim 53, wherein the authentication process verifies validity of the medium identification information with respect to an information recording medium which records a digital signature of a manufacturer for the information recording medium as a digital signature for a recording person of the medium identification information based on the manufacturer's digital signature.

55. The information recording method according to claim 53, wherein the authentication process performs authentication processing with respect to an information recording medium which records a revocation list about a recording person together with the authentication data based on the revocation list.

56. The information recording method according to claim 55, wherein the authentication process stores a revocation list recorded on an information recording medium when this revocation list is valid and is newer than the already stored revocation list, and performs authentication processing based on the newly stored revocation list.

57. An information playback method for playing back information from an

information recording medium including a random-pattern-information recording part for recording random pattern information based on random physical phenomena and an authentication data recording part for storing, as authentication data, medium identification information created according to random pattern information detected from the random-pattern-information recording part, wherein the information playback method, comprising:

a random-pattern-information detection process which detects random pattern information from a random-pattern-information recording part on an information recording medium;

a verification data creation process which creates medium-identification-information verification data from random pattern information detected by the random-pattern-information detection process;

an authentication process which reads authentication data from the authentication data recording part on an information recording medium and performs authentication processing for an information recording medium based on medium-identification-information verification data created by the verification data creation process and based on the authentication data; and

a playback control process which provides control of reading information from an information recording medium.

58. The information playback method according to claim 57, wherein the playback control process provides control of reading encrypted information from the

authenticated information recording medium, and

wherein the decryption process decrypts encrypted information read by the playback control process from an information recording medium by using medium identification information on an information recording medium authenticated by the authentication processing.

59. The information playback method according to claim 58, wherein the playback control process provides control of reading encrypted information and the encryption key used for information encryption from the authenticated information recording medium.

60. The information playback method according to claim 59, wherein the playback control process provides control of reading encrypted information and the encrypted encryption key from the information recording medium, and

wherein the decryption process decrypts a read and encrypted encryption key by using medium identification information on an information recording medium authenticated by the authentication processing and decrypts encrypted information by using the encryption key which was encrypted and information thereof is decrypted.

61. The information playback method according to claim 57, wherein the authentication process verifies validity of the medium identification information with respect to an information recording medium which records, as authentication data, the medium identification information together with a digital signature of a recording person who recorded the medium identification information based on the recording

person's digital signature, and performs authentication processing with respect to an information recording medium based on medium-identification-information verification data created by the verification data creation process and based on verified valid medium identification information.

62. The information playback method according to claim 61, wherein the authentication process verifies validity of the medium identification information with respect to an information recording medium which records a digital signature of a manufacturer for the information recording medium as a digital signature for a recording person of the medium identification information based on the manufacturer's digital signature.

63. The information playback method according to claim 61, wherein the authentication process performs authentication processing with respect to an information recording medium which records a revocation list about a recording person together with the authentication data based on the revocation list.

64. The information playback method according to claim 63, wherein the authentication process stores a revocation list recorded on an information recording medium in the storage part when this revocation list is valid and is newer than the already stored revocation list, and performs authentication processing based on the newly stored revocation list.

65. An authentication data recording method for recording authentication information on an information recording medium, comprising:

a random-pattern-information detection process which detects random pattern information from a random-pattern-information recording part on an information recording medium storing random pattern information based on random physical phenomena;

a medium identification information creation process which creates medium identification information from the random pattern information detected by the random-pattern-information detection process; and

an authentication data recording control process which provides control of recording, as authentication data, the medium identification information created by the medium identification information creation process in an authentication data recording part on the information recording medium.

66. The authentication data recording method according to claim 65, wherein the authentication data recording control process records, as authentication data, the medium identification information together with a digital signature for a recording person of the medium identification information in an authentication data recording part on the information recording medium.

67. The authentication data recording method according to claim 66, wherein the authentication data recording control process records a digital signature for a manufacturer of the information recording medium as a digital signature for a recording person of the medium identification information.

68. The authentication data recording method according to claim 65, wherein the

authentication data recording control process records a revocation list about a manufacturer together with the authentication data in an authentication data recording part on the information recording medium.

69. An authentication processing method for performing authentication processing with respect to an information recording medium, comprising:

a random-pattern-information detection process which detects random pattern information from a random-pattern-information recording part on an information recording medium;

a verification data creation process which creates medium-identification-information verification data from random pattern information detected by the random-pattern-information detection process; and

an authentication process which reads authentication data from the authentication data recording part on an information recording medium and performs authentication processing for an information recording medium based on medium-identification-information verification data created by the verification data creation process and based on the authentication data.

70. The authentication processing method according to claim 69, wherein the authentication process verifies validity of the medium identification information with respect to an information recording medium which records, as authentication data, the medium identification information together with a digital signature of a recording person who recorded the medium identification information based on the recording

person's digital signature, and performs authentication processing with respect to an information recording medium based on medium-identification-information verification data created by the verification data creation process and based on verified valid medium identification information.

71. The authentication processing method according to claim 70, wherein the authentication process verifies validity of the medium identification information with respect to an information recording medium which records a digital signature of a manufacturer for the information recording medium as a digital signature for a recording person of the medium identification information based on the manufacturer's digital signature.

72. The authentication processing method according to claim 70, wherein the authentication process performs authentication processing with respect to an information recording medium which records a revocation list about a recording person together with the authentication data based on the revocation list.

73. The authentication processing method according to claim 72, wherein the authentication process stores a revocation list recorded on an information recording medium in the storage part when this revocation list is valid and is newer than the already stored revocation list, and performs authentication processing based on the newly stored revocation list.

74. The authentication processing method according to claim 72, wherein the authentication process stores a recording person's identification information and a

public key thereof for a manipulated information recording medium together with a revocation flag, updates the revocation flag using a new revocation list, and performs authentication processing based on the revocation list stored in the storage process.

75. An information recording medium for recording information, comprising:

a random-pattern-information recording part which records random pattern information based on random physical phenomena;

an authentication data recording part which stores, as authentication data, medium identification information created according to random pattern information detected from the random-pattern-information recording part; and

an information recording part which records information.

76. The information recording medium according to claim 75, wherein the authentication data recording part records the medium identification information as authentication data together with a digital signature for a recording person of the medium identification information.

77. The information recording medium according to claim 76, wherein the authentication data recording part records a digital signature for a manufacturer of the information recording medium as a digital signature for a recording person of the medium identification information.

78. The information recording medium according to claim 77, wherein the authentication data recording part records a revocation list about a manufacturer together with the authentication data.